The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
https://www.us-cert.gov/tlp/

DATE(S) ISSUED:
05/18/2017

SUBJECT:
A Vulnerability in Joomla! Could Allow for SQL Injection

OVERVIEW:
A vulnerability has been discovered in Joomla!, which could allow for SQL Injection. Joomla! is an open source content management system for websites. Successful exploitation of this vulnerability could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- Joomla! versions prior to 3.7.1

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Joomla!, which could allow for SQL injection. This vulnerability exists due to inadequate filtering of request data in URL parameters. An attacker can exploit this issue by manipulating the SQL query logic in the URL bar in order to run SQL queries on the underlying database. (CVE-2017-8917) Successful exploitation of this vulnerably could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate patches provided by Joomla! to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:
Joomla!:
https://developer.joomla.org/security-centre/692-20170501-core-sql-injection.html

Sucuri:
https://blog.sucuri.net/2017/05/sql-injection-vulnerability-joomla-3-7.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8917